



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/614,982	07/12/2000	John R. Hind	5577-199	2459

20792 7590 05/07/2004
MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER

ADAMS, JONATHAN R

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 05/07/2004

3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/614,982

Applicant(s)

HIND ET AL.

Examiner

Jonathan R Adams

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07/12/2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-57 and 77 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other: _____

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
 - I. Claims 1-57 and 77 drawn to controlling updates to programmable memory within a device, classified in class 713, subclass 200.
 - II. Claims 58-76, 78, and 79 drawn to distributing updates to a plurality of generic processing devices, classified in class 717, subclass 177.
2. The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I has separate utility such as controlling updates obtained by means other than that of invention II. See MPEP § 806.05(d).
3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.
4. During a telephone conversation with O'SULLIVAN, TIMOTHY J. on 4/21/04 a provisional election was made without traverse to prosecute the invention of group 1, claims 1-57 and 77. Affirmation of this election must be made by applicant in replying to this Office action. Claims 58-76, 78, and 79 withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 21 and 36-38 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 21 recites the limitation "rules information" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 36 is self-dependent and is therefore of improper dependant form.

Claims 37 and 38 rejected as being dependent on an improper base claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 22 and 27 rejected under 35 U.S.C. 102(b) as being preceded by Bealkowski et al., US Patent No. 5022077 (hereafter referred to as '077).
9. As to claim 22:

Art Unit: 2134

'077 teaches a method to prevent unauthorized changes to BIOS (Col 3, Line 10, '077) comprising:

Latch/latch enable circuit/memory controller allows write access to programmable memory after hardware reset / In response to a reset signal the protection means permits access to the protected region (Col 3, Line 26, '077)

Latch/latch enable circuit/memory controller prevents write access to programmable memory upon completion of memory update window / Bios generates a second signal which activates a protection means to prevent access to the region on the disk containing the master boot record and the BIOS image (Col 3, Line 31 et seq., '077)

10. As to claim 27:

Latch/latch enable circuit/memory controller allows read access to programmable memory after hardware reset / In response to a reset signal the protection means permits access to the protected region (Col 3, Line 26, '077)

Latch/latch enable circuit/memory controller prevents read access to programmable memory upon completion of memory update window / Bios generates a second signal which activates a protection means to prevent access to the region on the disk containing the master boot record and the BIOS image (Col 3, Line 31 et seq., '077)

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 1-20, 39-57, and 77 rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, US Patent NO. 5844986(hereafter referred to as '986) in view of '424.

13. As to claims 1 and 39:

'986 teaches a method for providing secure BIOS firmware updates. '986 does not teach to only allow access to the programmable memory during an update window of authorized access. '424 teaches several security strategies to protect access to a programmable memory, including the use of an authorized access window of predefined duration (Col 5, Line 55, '424). It would have been obvious to a person of ordinary skill in the art at the time of invention employ the security strategies of '424 with the secure BIOS update system of '986. One of ordinary skill in the art would have been motivated to employ the security strategies of '424 with the secure BIOS update system of '986 because utilizing additional security strategies helps to reduce potential security vulnerabilities.

14. As to claims 2 and 40:

Allowing access to programmable memory based on access latch / If the new BIOS is valid... the previous BIOS program is deleted (Col 4, Line 14, '986). It is inherent that

Art Unit: 2134

the validity variable used in '986 is stored in a memory latch, because this is the way by which computers process information.

Setting the access latch to allow access after a hardware reset / All BIOS functions take place after a hardware reset

Executing an update control program (UCP) / Cryptographic Coprocessor performs authentication, validation (Col 2, Line 61, '986), and BIOS replacement (Col 3, Line 49, '986) operations.

Resetting the latch to prevent access upon completion of the UCP / the validity variable is used only with the BIOS replacement operation.

15. As to claims 3 and 41:

Allowing/Preventing access to a memory where the update control program resides based on access latch / If the new BIOS is valid... the previous BIOS program is deleted (Col 4, Line 14, '986). It is inherent that the validity variable used in '986 is stored in a memory latch, because this is the way by which computers process information. Cryptographic coprocessor contains the BIOS firmware (Col 2, Line 59, '986)

16. As to claims 4, 6, 42, and 44:

Determine if an update is available (based on status information) / Actively receives new BIOS program code from a specified source (Col. 3, Line 56, '986)

Art Unit: 2134

Update programmable memory if update is available / the new BIOS is stored internally (Col. 3, Line 58, '986), New BIOS program is made operational (Col 4, Line 14, '986)

17. As to claims 5 and 43:

Determining step examines local memory, local drive, network drive, or input device status / Crypto-coprocessor actively retrieves it from a specified source (eg. system memory) (Col. 3, Line 56, '986), Users download upgrade via Internet (Col 3, Line 43, '986)

18. As to claims 7 and 45:

Obtaining an update image / Actively receives new BIOS program code from a specified source (Col. 3, Line 56, '986)

Obtaining installation information from update image / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986)

Writing update data to programmable memory / The new BIOS program is stored internally (Col. 3, Line 58, '986)

19. As to claims 8 and 46:

'986 as modified above teaches a method for providing secure BIOS system driver updates assisted by a BIOS management utility software. '986 does not specifically teach for the BIOS management utility software to be obtained via

Art Unit: 2134

download. The examiner takes official notice as to obtain the BIOS management utility software with BIOS upgrade via download. It would have been obvious to a person of ordinary skill in the art at the time of invention to obtain the BIOS management utility software with BIOS upgrade via download. One of ordinary skill in the art would have been motivated to obtain the BIOS management utility software with BIOS upgrade via download because it is customary to make Internet upgrades available with an installation program. Examples include Microsoft Windows upgrades and peripheral device driver upgrades, etc.

20. As to claims 9 and 47:

Loading update image temp workspace / First storage element for storing a code update, a second storage element for storing the executable code that needs to be updated (Col. 2, Line 11, '986)

21. As to claims 10 and 48:

Storing existing data to provide a backup copy / A second storage element for storing the executable code that needs to be updated (Col. 2, Line 11, '986)

22. As to claims 11 and 49:

Determining if the update was successful, restoring use of the backup copy/ If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and never used (Col 4, Line 13, '986)

23. As to claims 12 and 50:

Verifying the authenticity of the update / Cryptographic coprocessor performs the appropriate authentication operations on the new BIOS program (Col. 3, Line 61, '986)

24. As to claims 13 and 51:

Evaluate at least one certificate... valid digital signature / Using the well known techniques of digital signatures and certificates to validate the integrity and validity of the new BIOS program (Col. 4, Line 1, '986)

25. As to claims 14 and 52:

Decrypt the digital signature using a shared secret / authentication can be preformed... by the use of secret information (Col. 3, Line 65, '986)

26. As to claims 15 and 53:

Decrypting a digital signature using a public key... comparing with precomputed value / public/private key cryptography... using techniques of digital signatures (Col. 3, Line 67, '986)

27. As to claims 16 and 54:

Public key is stored in a non-updateable memory / Cryptographic coprocessor will be preloaded with the public key (Col 4, Line 31, '986)

28. As to claims 17 and 55:

Provide public key in previous versions... obtain public key from programmable memory / Cryptographic coprocessor may be preloaded with another public key that may be used to authenticate a certificate chain to obtain this industry association public key (Col 4, Line 34 et seq., '986)

29. As to claims 18 and 19:

Hierarchical plurality of certificates / certificate chain (Col 4, Line 36, '986)

30. As to claims 20 and 56:

Obtaining/evaluating application rules information from certificate associated with update / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986)

31. As to claims 57:

Evaluating rules information associated with one of: manufacturer of the device ... / Certificate associated with manufacturer (Col 2, Line 49, '986)

32. As to claims 77:

Claim 77 corresponds to claim 2.

33. Claims 23, 24, and 25 rejected under 35 U.S.C. 103(a) as being unpatentable over '077 in view of Christeson et al., US Patent No. 5579522 (hereafter referred to as '522).

34. As to claim 23:

'077 teaches a hardware implementation (Fig 2) of a method to prevent unauthorized changes to BIOS (Col 3, Line 10, '077) upon completion of the memory access window started at reset. '077 does not teach a read only memory containing a program associated with a processor to update the programmable memory. '522 teaches the use of a read only recovery BIOS with recovery update functionality for updating a corrupted system BIOS (Col 6, Line 30 et seq., '522) . It would have been obvious to a person of ordinary skill in the art at the time of invention to use the recovery BIOS with recovery update feature of '522 in addition to the protected BIOS system in '077. One of ordinary skill in the art would have been motivated to use the recovery BIOS with recovery update feature of '522 in addition to the protected BIOS system in '077 because doing so would protect the system of '077 from being inoperable in the event that the system BIOS has been corrupted.

35. As to claim 24:

Executing the program contained in the read only memory upon generation of the hardware reset / Upon power up or reset, the processor jumps to a location within the protected recovery BIOS block (Col 3, Line 18, '522)

36. As to claim 25:

Set the latch to the second state upon completion of execution of the program / Bios generates a second signal which activates a protection means to prevent access to the region on the disk containing the master boot record and the BIOS image. Bios then boots the operating system (Col 3, Line 31 et seq., '077). It would be necessary to prevent access to the newly updated system BIOS to ensure the further protection upon completion of the recovery BIOS/update and transfer of system control to the operating system.

37. Claim 26 rejected under 35 U.S.C. 103(a) as being unpatentable over '077 in view of '522 in further view of "Introduction to Digital Signal Processors" (hereafter referred to as DSP).

38. As to claim 26:

'077 as modified above teaches hardware implementation (Fig 2) of a method to prevent unauthorized changes to BIOS (Col 3, Line 10, '077) utilizing a 80386 PC processor. Not specifically taught is for the processor to comprise a digital signal processor. DSP teaches a Pentium PC processor with MMX. It would be obvious to a person of ordinary skill in the art to use the more modern Pentium processor with MMX in place of the 80386 exemplified in '077. One of ordinary skill in the art would have been motivated to the more modern Pentium processor with MMX in place of the 80386

Art Unit: 2134

exemplified in '077 because the Pentium MMX series of processors provides similar functionality and greater speed to that of the 80386.

39. Claims 28-35 rejected under 35 U.S.C. 103(a) as being unpatentable over '077 in view of '986.

40. As to claims 28 and 30:

'077 teaches a hardware implementation of a method to prevent unauthorized changes to BIOS (Col 3, Line 10, '077) upon completion of the memory access window started at reset. '077 does not teach to determine (based on status information) if a BIOS update is available then update the BIOS. '986 teaches a method for actively receiving and securely updating BIOS firmware. It would have been obvious to a person of ordinary skill in the art at the time of invention to use the BIOS updating means of '986 with the BIOS protection means of '077. One of ordinary skill in the art would have been motivated to use the BIOS updating means of '986 with the BIOS protection means of '077 because field updating of BIOS firmware can help to correct programming errors or corrupted copies of the existing BIOS.

41. As to claim 29:

Determine if an update is available by examining local memory, local drive, network drive, or input device status / Crypto-coprocessor actively retrieves it from a specified source (eg. system memory) (Col. 3, Line 56, '986), Users download upgrade via Internet (Col 3, Line 43, '986)

42. As to claim 31:

Obtaining an update image / Actively receives new BIOS program code from a specified source (Col. 3, Line 56, '986)

Obtaining installation information from update image / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986)

Writing update data to programmable memory / The new BIOS program is stored internally (Col. 3, Line 58, '986)

43. As to claim 32:

BIOS updating means of '986 with the BIOS protection means of '077

'077 as modified above teaches a BIOS protection means providing secure BIOS system driver updates assisted by a BIOS management utility software. '077 as modified above not specifically teach for the BIOS management utility software to be obtained via download. The examiner takes official notice as to obtain the BIOS management utility software with BIOS upgrade via download. It would have been obvious to a person of ordinary skill in the art at the time of invention to obtain the BIOS management utility software with BIOS upgrade via download. One of ordinary skill in the art would have been motivated to obtain the BIOS management utility software with BIOS upgrade via download because it is customary to make Internet upgrades

Art Unit: 2134

available with an installation program. Examples include Microsoft Windows upgrades and peripheral device driver upgrades, etc.

44. As to claim 33:

Loading update image temp workspace / First storage element for storing a code update, a second storage element for storing the executable code that needs to be updated (Col. 2, Line 11, '986)

45. As to claim 34:

Storing existing data to provide a backup copy / A second storage element for storing the executable code that needs to be updated (Col. 2, Line 11, '986)

46. As to claim 35:

Determining if the update was successful, restoring use of the backup copy/ If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and never used (Col 4, Line 13, '986)

Conclusion


47. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703)

Art Unit: 2134

305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

48. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306

49. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100